LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

# Kansallisen tietoturvallisuuskorttikoulutuksen laatiminen

Hämäläinen, Leo

2015 Leppävaara

**Laurea-ammattikorkeakoulu**
Leppävaara

# Kansallisen tietoturvallisuuskorttikoulutuksen laatiminen

Hämäläinen Leo
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Joulukuu, 2015

**Laurea-ammattikorkeakoulu** **Tiivistelmä**
Leppävaara
Turvallisuusalan koulutusohjelma

Leo Hämäläinen

**Kansallisen tietoturvallisuuskorttikoulutuksen laatiminen**

Vuosi 2015 Sivumäärä 38

Opinnäytetyön aiheena on projekti jonka tavoitteena on tietoturvallisuuskorttikoulutuksen laatiminen turvallisuus- ja koulutusalan yritys Alertum Oy:lle. Opinnäytetyö on luonteeltaan konstruktiivinen jonka tavoitteena on luoda konkreettinen tuote tai palvelu, tässä tapauksessa tietoturvallisuuden korttikoulutusohjelma Alertum Oy:lle. Tässä opinnäytetyön raportissa kuvataan koulutusohjelman rakentamisprosessi, sekä sen edellyttämä taustatyö. Korttikoulutuksen sisältö laadittiin Alertum Oy:n vaatimusten ja rajausten mukaisesti.

Opinnäytetyö koostuu kahdesta osasta. Ensimmäinen osa on Alertum Oy:lle luotu tietoturvallisuuskorttikoulutusohjelma, ja toinen osa on tämä opinnäytetyöraportti.

Opinnäytetyöraportti sisältää lyhyesti selostetun tietoturvallisuuden tietoperustan. Opinnäytetyötä varten kerätty tausta-aineisto pohjautuu käräjäoikeudesta saatuihin pöytäkirjoihin, Viestintäviraston tietoturvallisuus-järjestelmistä saatuihin tilastoihin ja erinäisien asiantuntijoiden haastatteluihin. Tämä aineisto loi perustelun koulutusohjelman luomiselle, sekä sen tarpeellisuudelle Suomessa.

Opinnäytetyön aikana luodun varsinaisen koulutusohjelman tarkka sisältö on Alertum Oy:n liikesalaisuus, jonka takia sitä ei sisälletä osaksi opinnäytetyöraporttia otsikkotasoisia liitteitä ja yksittäisiä, havainnollistavia kuvia lukuun ottamatta.

Avainsanat
Tietoturvallisuus, turvallisuuskoulutus, riskienhallinta

**Laurea University of Applied Sciences** **Abstract**
Leppävaara
Security management Programme

Leo Hämäläinen

**Creation of a national information security card training programme**

Year 2015 Pages 38

The subject of this thesis is a project with the goal of creating an information security card – training program for Alertum plc. The form of the thesis is constructive, and its goal is to create a concrete product, the training program which will be used by Alertum plc. This thesis covers the process of creating the program, and the necessary research that went into the programs creation. The contents of the program were made according to the demands and specifications of Alertum plc.

The thesis consists of 2 parts. The first one is the created training program, and the second part is this report.

The thesis briefly covers the development of information security. It consists of material gathered from district courts, statistics gathered by various systems created by the Finnish Communications Regulatory Authority, and several specialist interviews. The content of this material both displays the necessity as well as underlays the rationale behind the topics chosen for the course.

The actual training program created during the thesis process is a trade secret of Alertum plc, and for that reason is not included as a part of this report, with the exception of singular, descriptive pictures and the table of contents of the topics covered by the training program.

Keywords

Information security, security training, risk management

Sisällysluettelo

# 1 Johdanto

Tietoturvallisuudessa on nimen mukaisesti kyse tiedosta ja sen turvaamisesta. Ilmiö ei ole pelkästään tietojenkäsittelyyn liittyviin järjestelmiin rajoittuva, vaan tarvetta rajoittaa tietoa vain sen näkemiseen oikeutetuille henkilöille on ollut läpi historian. Aikaisimmat esimerkit tietoturvallisuudesta koostuvat mm. paperisen materiaalin säilyttämistä kassakaapeissa tai muissa lukituissa tiloissa, sekä kirjoitetun tiedon salaamisesta erinäisillä kryptografisilla menetelmillä joista tunnetuin esimerkki on Rooman keisarin Julius Caesarin käyttämä, ja hänen mukaansa nimetty Caesar-salausmetodi (Savarese & Hart, 1999).

Myöhemmin tietojärjestelmien ja tiedonsiirron kehittyessä välitetyn tiedon turvaamisessa haasteet lisääntyivät. Viestiliikenteen kehittyessä ja monipuolistuessa tiedon turvaamista varten käyttöön tuli monia eri ratkaisuja. Kaukokirjoitinverkoissa kuten Telexissä oli sisäänrakennettuja viestin salausjärjestelmiä (Helsingin Sanomat, 2015). Analogisessa puheliikenteessä puolestaan 40-luvulta lähtien käytössä oli spektrin kääntöjärjestelmiä joissa lähetyspäässä taajuustason kääntäjä muutti puheen spektrin peilikuvaksi ja vastaanottajapäässä kääntäjä muutti sen takaisin normaaliksi. Tällä järjestelyllä liikennettä kuunteleva henkilö ei saanut selvää puheliikenteestä (Hämäläinen, 2015). Nykypäivän sähköpostiliikenteessä puolestaan käytetään turvapostin tapaisia ratkaisuja joissa lähetetty viesti salataan ja vastaanottajalle annetaan avain jolla viestin sisällön pystyy purkamaan. Trendinä jokaisessa näistä järjestelmistä on viestin lähettäjäpuolella tehty salaus ja vastaanottopuolella tapahtuva purku.

Nykypäivän tietoturvallisuuskoulutuksessa on kyse koko organisaation riskienhallintaan liittyvästä koulutuksesta. Tietoturvallisuus on osa yrityksen kokonaisturvallisuutta, jonka tavoitteena on turvata yrityksen henkilöstöä, mainetta, tietoja, omaisuutta ja ympäristöä (Elinkeinoelämän keskusliitto, 2015). Näistä kaikilla on välitön yhteys toiminnan jatkuvuuteen ja tietoturvallisuuteen. Asianmukaisesta tietoturvallisuudesta huolehtimalla pystytään sekä vähentämään tietomurroista johtuvia riskejä yritykselle, että minimoimaan siitä syntyviä vahinkoja (Valtionhallinnon tietoturvallisuuden johtoryhmä, 2011). Tietoturvallisuuden merkitys on selvästi kasvava trendi joka näkyy mm. valtion virastoihin kohdistuvissa urkinnoissa (Helsingin Sanomat, 2013), mutta toisaalta myös tavallisten kansalaisten, yritysten ja erinäisten organisaatioiden jokapäiväisessä elämässä. Tietoturvallisuudessa nykypäivänä kyseessä ei enää ole pelkästä välitetyn tai tallennetun tiedon suojaamisesta, vaan myös järjestelmien ja organisaation toimintakyvyn turvaamisesta (Valtion tieto- ja viestintätekniikkakeskus, 2014).

## 1.1 Tavoite

Tämän opinnäytetyön tavoitteena on luoda edellytyksiä tietoturvallisuuden parantamiseen valtakunnallisella tasolla. Käytännössä tämä tapahtuu Alertum Oy:lle luodulla tietoturvallisuuden korttikoulutusohjelmalla, sisältäen koulutusmateriaalin tuottamisen sekä muita koulutusohjelmaa tukevia tehtäviä ja materiaaleja. Koulutusta varten julkaistiin 19.10.2015 erillinen tietoturvallisuuskortti – sivusto joka tarjoaa tietoja koulutuksen sisällöstä, kustannuksista sekä aikatauluista sivuston etusivun kuvakaappaus on esitelty kuvassa 1. Opinnäytetyön luoman tietoturvallisuuskorttikoulutuksen mottona on ”Tietoturvallisempi Suomi”, koulutuksen ja opinnäytetyön tavoitteena on kasvattaa ymmärrystä ja sitä kautta tietoturvallisuuden tasoa Suomessa parantamalla Suomalaisten tietoisuutta tietoturvallisuuteen liittyvistä riskeistä, sekä tarjota perustiedot ja taidot yleisimpien tietoturvallisuuteen liittyvien uhkien torjumiseksi.


Kuva 1. Kuvakaappaus Tietoturvallisuuskortti.fi – sivustolta

Taustalla opinnäytetyössä on Alertum Oy:n tavoite luoda valtakunnallinen tietoturvallisuuden lyhytkoulutusohjelma jonka kohteena on yksittäisien tietoturvahenkilöiden ja asiantuntijoiden sijasta laajempi yleisö eli koko organisaatio. Viestintävirastolta saaduista tilastoista, Espoon- sekä Helsingin käräjäoikeuksien tuomiopöytäkirjoista, että Keskusrikospoliisin Kyberrikostorjuntakeskuksen päällikkö Timo Piiroisen haastattelun pohjalta voitiin todeta selkeä tarve perustason koulutukselle.

Iso osa tietoturvahyökkäyksistä tapahtuu yksinkertaisia hyökkäystapoja hyödyntäen ja ovat täten kustannustehokkaasti torjuttavissa henkilöstön perustasoisella kouluttamisella. Yleisimmät uhat kuten sähköpostien liitetiedostot tai epäilyttävät linkit ovat metodeja joilla organisaation tietoihin pyritään pääsemään käsiksi, ja joita organisaatiot kohtaavat nykypäivänä

viikoittain. Käyttäjän toimista riippuen, nämä yksittäiset metodit voivat antaa haittaohjelmille tai ulkopuolisille tahoille pääsyn ensin käyttäjän laitteistoon ja usein siitä edelleen koko laiteverkkoon (Piiroinen, 2015).

## 1.2 Kehityskohteeseen liittyvää problematiikkaa

Suomessa tilastotietojen hankkiminen tietoturvallisuuteen liittyvästä rikollisuudesta on toistaiseksi haasteellista johtuen osittain tietoturvallisuuteen liittyvien rikosten nimikkeistä (Piiroinen, 2015). Vaikka joillain organisaatioilla on sähköisen viestinnän tietosuojalain pohjalta ilmoitusvelvollisuus tietoturvaloukkauksista, koskee ilmoitusvelvollisuus vain Viestintävirastolle ilmoittamista. Viestintävirasto käsittelee tiedot luottamuksellisesti ja antaa suosituksia, mutta ei pysty pakottamaan rikosilmoituksen tekoon, jolloin tietoturvallisuusrikokset eivät välttämättä tule poliisin tietoon ja käsittelyyn.

Luvaton käyttö sekä maksuvälinepetos ovat esimerkkejä syytteistä, joita käytetään tietoturvarikollisuudesta epäiltyjen syyttämiseksi, mutta sisältävät myös muita rikollisuuden muotoja kuten ajoneuvovarkauksia tai väärennetyn rahan käyttöä. Tästä johtuen todellisen tietoturvarikollisuuden määrää Suomessa ei voida tilastoida yksin poliisiammattikorkeakoulun ylläpitämän PolStat-tietokannan tilastotiedoista (Piiroinen, 2015). Yhtenä merkittävimmistä tilastotiedon keruumetodeista on tämän vuoksi Viestintäviraston autoreporter – järjestelmä joka tilastoi Suomesta lähtöisin olevaa haittaohjelmaliikennettä, sekä analysoi ja luokittelee haittaohjelman sekä sen alatyypin. Autoreporterin toimintaperiaatteena on haittaohjelmien lähettämän tietoliikenteen analysointi ja kategorisointi. Tämä on toisaalta tehokas ja automatisoitu tiedonkeruumetodi, mutta järjestelmän ongelmana ovat haittaohjelmat, kuten tietokoneiden kovalevyjä salaavat kiristysohjelmat, jotka eivät lähetä tietoliikennettä saastutettuaan järjestelmiä ja jäävät täten autoreporterin tilastojen ulkopuolelle.

Autoreporterin luomien tilastojen avulla voidaan kuitenkin havainnoida että suuri osa tietoturvahyökkäyksistä tapahtuu yksinkertaisia ja pitkään käytössä olleita metodeja käyttäen. Nämä hyökkäystyypit pyrkivät usein ohittamaan tietoturvajärjestelyjä ohjaamalla kohdehenkilöä toimimaan näitä järjestelyjä ohittaen. Tällaisen toiminnan estäminen ei ole mahdollista pelkällä laitteistolla, vaan edellyttää organisaatiossa henkilöstön koulutusta tunnistamaan mahdollisia uhkia, sekä opettamaan heille oikeita toimintatapoja niiden välttämiseksi.

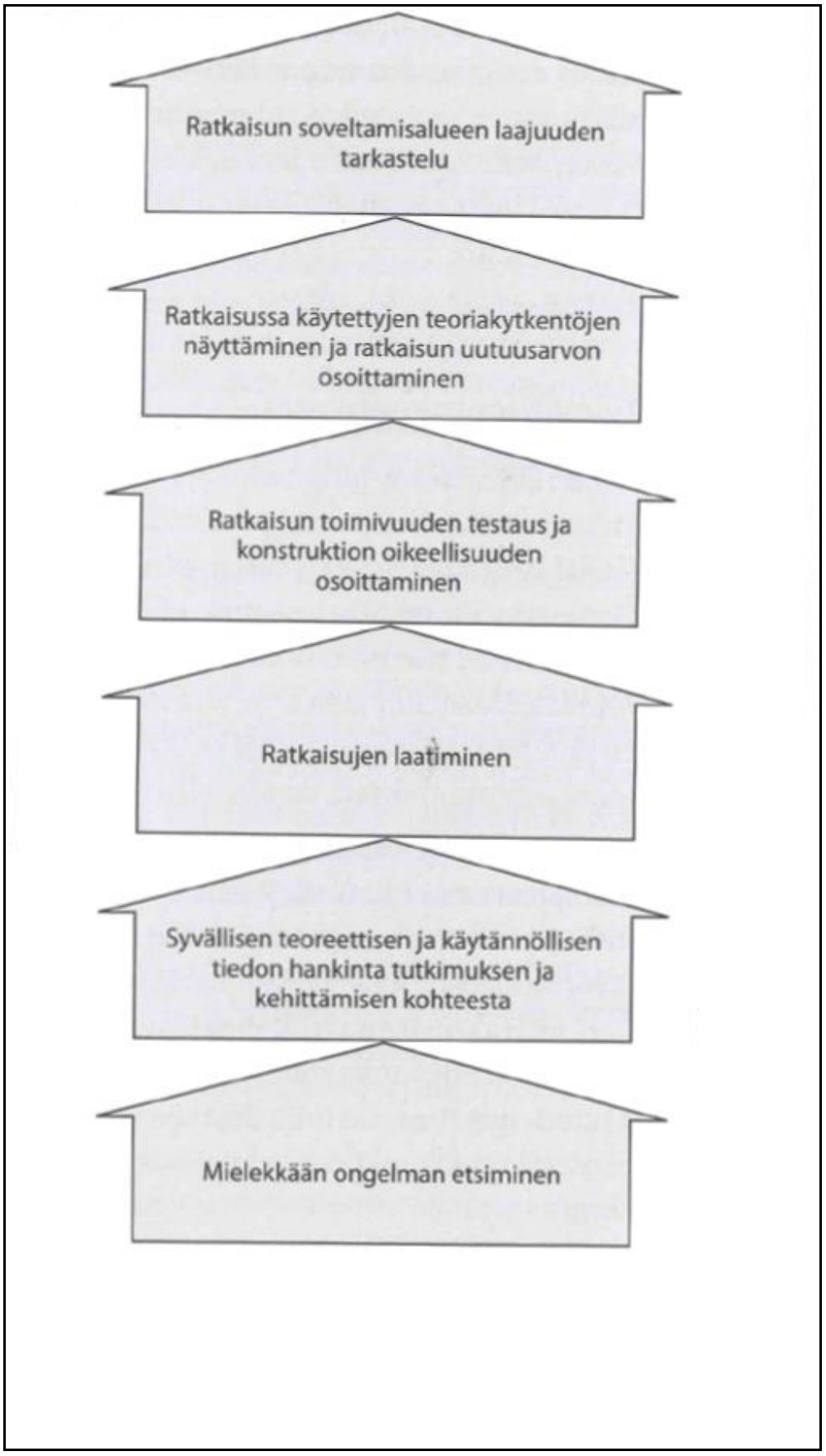
## 1.3 Rajaus

Koska opinnäyteyön aiheena on uuden koulutusohjelman luominen kohdeorganisaatiolle, on koulutusohjelman muodon ja sisällön rajaus tullut suoraan kohdeorganisaatiolta. Koska Opinnäytetyö on konstruktiivinen, tulee työn luoda teoreettisesti perusteltu käytännön ratkaisu ongelmaan. Tässä työssä ongelma on Tietoturvallisuuden yleinen taso Suomessa ja ratkaisuna koko organisaation henkilöstölle kohdistettu Tietoturvallisuuskorttikoulutus jonka sisältö perustuu saatavilla oleviin tilastoihin, asiantuntijalausuntoihin sekä Alertum Oy:n tekemiin asiakaskyselyihin. Työn rajaus kohdistuu näiden pohjalta konkreettiseen tuotteeseen, eli tietoturvallisuuskorttikoulutuksen luomiseen Alertum Oy:lle, ja koulutuksen sisällön perusteluun tietoturvallisuuden näkökulmasta. Tietoturvallisuuskorttikoulutuksen varsinainen rakenne on myös rajattu Alertum Oy:n toimesta lyhytmuotoiseksi aikuiskoulutukseksi. Koulutuksen sisällön koostumus on edelleen rajattu tietoturvallisuuden peruskäsitteistöön ja käytännön toimenpiteisiin ja esimerkkitapauksiin.

Opinnäytetyössä ei oteta kantaa muihin tietoturvallisuuden ratkaisuihin, kuten kulunvalvontaan, auditointiin tai teknisiin ratkaisuihin ellei niitä ole ollut tarpeen miettiä osana koulutuksen sisältöä. Koulutuksessa ei myöskään ole tarkoituksenmukaista miettiä esimerkiksi CISSP-standardien mukaisia erittäin teknisiä ja monimutkaisia, tietoturva-asiantuntijoille tarkoitettuja koulutussisältöjä tai järjestelmien teknistä puolta sen enempää kuin se on välttämättömästi tarpeellista työntekijän näkökulmasta perusasioiden sisäistämiseksi. Koulutusohjelman runko tuli myös kohdeorganisaatiolta, käsittäen sekä lähiopetuksen että sähköisen, esitäytetyn verkkomoduulin, jonka tarkoituksena on tehostaa lähiopetusta kokopäiväisestä puolipäiväiseksi. Tämä palvelee yrityksien tarpeita, jolloin henkilöstön osallistuminen kurssille ei vaadi suurta panostusta. Tuotettu materiaali on rajoittunut koulutuspalvelun ympärille. Opinnäytetyö ei myöskään ota kantaa turvallisuuskoulutukseen tai sen pedagogisiin näkökulmiin muilta kuin varsinaista tietoturvallisuuskorttikoulutusta koskien.

## 1.4 Metodologia

Opinnäytetyö on muodostettu Konstruktiivisen tutkimuksen prosessin mukaisesti. Prosessi on jaettu kuuteen osaan, koostuen Mielekkään ongelman etsimisestä, syvällisen teoreettisen ja käytännöllisen tiedon hankinnasta tutkimuksen ja kehittämisen kohteesta, ratkaisujen laatimisesta, ratkaisun toimivuuden testauksesta ja konstruktion oikeellisuuden osoittamisesta, ratkaisussa käytettyjen teoriakytkentöjen näyttämisestä ja ratkaisun uutuusarvon osoittamisesta sekä ratkaisun soveltamisalueen laajuuden tarkastelusta (Kasanen Lukka, & Siitoinen 1991, 301–329). Tämä prosessijako on selvennettynä kuvassa 2.




Kuva 2. Konstruktiivisen opinnäytetyön prosessi

Vaikka tämä järjestys on tehty lineaariseksi, oli Projektin tiukasta aikataulusta johtuen kehitysprosessin osia valmisteltava osittain rinnakkain. Opinnäytetyön tekeminen aloitettiin kesäkuussa, ja koulutusohjelman luominen saatettiin loppuun marraskuussa jolloin järjestettiin pilottikoulutukset sekä koulutusohjelman lanseeraustilaisuus. Toisaalta myös mielekkään ongelman etsiminen ja tutkimuksen taustatietojen kartoitus ei ollut tarpeen sillä ongelma, ja osa taustatiedoista tulivat suoraan Alertum Oy:ltä. Opinnäytetyön oikeellisuuden arviointi perustuu työelämän vaikuttavuusarvioon jonka on kirjoittanut Alertum Oy:n johtava turvallisuusasiantuntija ja osakas Lari Linden.

## 1.5 Tietoturvallisuuden teoriapohja ja työssä käytetty aineisto

Teoriapohjan opinnäytetyössä muodostaa erinäiset tietoturvallisuuteen liittyvät julkishallinnon organisaatioiden tuottamat materiaalit joista keskeisimmät ovat Kansallinen auditointikriteeristö KATAKRI sekä Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI – ohjeisto. Näiden lisäksi verrannaismateriaalina käytössä oli erinäisiä CISSP-koulutusmateriaaleja sekä International Organization for Standardization – organisaation ISO/IEC 27000 Tietoturvallisuuden hallinta ja ISO 31000 riskienhallinta – standardeja. Verkkokoulutuksen pohjana käytettiin myös Granite Partners Oy:n luomia verkkokoulutusmateriaaleja. Pedagogisena näkökulmana koulutuksen sisällön muotoilua ja esittämistä mietittiin yhdessä Alertum Oy:n koulutuspäällikkö Mika Aholan kanssa jonka kanssa päädyttiin pohjaamaan koulutusta konstruktiivisen oppimiskäsityksen mukaisesti. Koulutuksen pedagogiikasta ja metodologiasta on erillinen kappale 3.1 joka käsittelee aihetta tarkemmin.

Käytetty aineisto koostuu poliisiammattikorkeakoulun ylläpitämään PolStat-tilastojärjestelmän, Viestintäviraston autoreporter- ja HAVARO-järjestelmien tilastotiedoista, tietoturvallisuuteen liittyvien oikeustapausten tuomiopöytäkirjoista, asiantuntijahaastatteluista, Viestintäviraston asiantuntijakyselyistä että Alertum Oy:ltä saaduista tiedoista. Autoreporter, ja HAVARO- järjestelmiä sekä PolStatin tilastojärjestelmää esitellään tarkemmin keskeisien käsitteiden osiossa. Julkisista lähteistä tilastotietoa on saatavilla hyvin vähän johtuen edellä mainituista syistä kuten saman rikosnimikkeen käytöstä sekä tietoturvarikollisuuteen että muuhun rikollisuuteen liittyen, että varsinaisen toiminnan kokoluokasta. HAVARO-järjestelmän kohdalla tilastoja ei luovuteta ulkopuolisille julkisia yksittäisiä raportteja johtuen huoltovarmuusorganisaatioiden toimintaan liittyvistä salassapitojärjestelyistä.

Yksittäisistä tilastoista Suomessa ei pystytä päättelemään tarkkaa toiminnan kokoluokkaa, vaan tietoturvallisuuskoulutusta luodessa rakennettiin samalla oma tilasto, jossa käytettiin sekä poliisin Polstat, että Viestintäviraston autoreporter, ja HAVARO – järjestelmien tilastoja kokonaiskuvan määrittämiseksi. Tämän kokonaiskuvan ja asiantuntijoiden henkilöhaastattelujen pohjalta päätettiin koulutuksen rakenne, jonka tukena käytettiin esimerkkitapauksia ja

valtionhallinnon olemassa olevia ohjeita sekä käytäntöjä. Näiden ohella arvoitiin myös ISO 31 000 ja 27 000 – standardien kriteerejä ja sisältöä tietoturvallisuuteen liittyvään koulutukseen nähden.

## 1.6 Keskeiset käsitteet

**Tietoturvallisuus**

”Tietoturvajärjestelyjen tarkoituksena on varmistaa tietoaineistojen, tietojärjestelmien ja palveluiden asianmukainen suojaus siten, että niiden luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit otetaan huomioon” (Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä, 2013)

**Tietoturvallisuuskorttikoulutus**

On opinnäytetyön aikana luotu, koko organisaatiolle tarkoitettu lyhytkoulutusjärjestelmä. Koulutus on suunniteltu vastaamaan henkilöstön tietoturvallisuusosaamisen viranomaisohjeisiin ja suosituksiin ja on yhtenäinen tapa osoittaa organisaation henkilöstön olevan perehdytetty toimimaan tietoturvallisuuden periaatteiden mukaisesti. Koulutus on kaksiosainen ja koostuu esitäytettävästä verkkomoduulista joka sisältää tentin, sekä neljän tunnin lähiopetuksesta, että käytännön harjoitteista (Alertum Oy, 2015).

**KATAKRI**

”KATAKRI on viranomaisten auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. KATAKRIin on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset.

KATAKRI itsessään ei aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. KATAKRIssa esitettyjen vaatimusten yhteyteen on merkitty lähdeviittaus läpinäkyvyyden varmistamiseksi” (Puolustusministeriö, 2015).

**VAHTI**

”On Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTIn ohjeisto. VAHTIn tietoturvaohjeisto on yksi maailman kattavimmista yleisistä tietoturvaohjeistoista. VAHTI-ohjeita käytetään hallinnon lisäksi laajasti hyväksi myös kansainvälisessä tietoturva- ja yhteistyössä, elin-

keinoelämässä, yrityksissä ja kunnissa sekä opetus- ja kansalaistoiminnassa” (Valtionvarainministeriö, 2015).

**CISSP**

On $(ISC)^2$ – organisaation luoma Certified Information Systems Security Professional – tietoturvatutkintosertifikaatti jonka kohdeyleisönä ovat tietoturvallisuuden kanssa toimivat asiantuntijat kuten tietoturva-vastaavat, verkkoarkkitehdit tai tietoturvallisuus-auditoijat. CISSP on yksi kattavimmista ja kansainvälisesti tunnetuimmista tietoturvallisuuteen liittyvistä tutkintosertifikaateista.

**HAVARO**

On julkishallinnon tarjoama, huoltovarmuuskriittisille yrityksille ja toimijoille suunnattu tietoturvaloukkausten havainnointi- ja varoituspalvelu jossa seurataan yritykseen tulevaa ja sieltä lähtevää internetpohjaista tietoliikennettä. Sen sisältämän tiedon avulla pyritään havaitsemaan tietoturvaan vaikuttavat ilmiöt mahdollisimman varhaisessa vaiheessa, jotta tarvittavat suojaustoimenpiteet voidaan aloittaa ajoissa ja suunnata oikein. (Huoltovarmuuskeskus, 2014)

**PolStat**

”PolStat on poliisiammattikorkeakoulun ylläpitämä tulostietojärjestelmä. PolStat-järjestelmän avulla tuotetaan tilastoja ja raportteja poliisin toiminnasta. PolStat sisältää tietoa monista eri tietojärjestelmistä, ja se on tietovarasto poliisille ja ulkopuolisille tiedontarvitsijoille” (Poliisiammattikorkeakoulu, 2015).

**Autoreporter**

On Viestintäviraston Kyberturvallisuuskeskuksen luoma palvelu jonka tarkoituksena on edistää tietoverkkojen puhtautta Suomessa. poistamalla haittaohjelmia sekä haitallista liikennettä lähettäviä tahoja. Autoreporterin toiminta perustuu tiedonkeruuseen jossa Suomesta lähtevään haittaohjelmaliikennettä kerätään lähes kaikkialta maailmasta. Autoreporter ei kerää tietoa haittaohjelmista jotka eivät lähetä tietoliikennettä eteenpäin saastuneesta koneesta, joten tilastojen keräämisessä joudutaan käyttämään muita tietolähteitä. Tiedot välitetään liittymiä ylläpitäville teleyrityksille, jotka ilmoittavat havainnoista asiakkailleen. Autoreporterin keräämää tietoa on saatavilla raakaversiona, josta on anonymisoitu haittaliikennettä lähettävien laitteiden IP-osoitteet sekä teleyrityksien pyynnöstä AS-numero. Dataan kuuluu

liikenteen alku- ja loppuajankohdat, kaupunkitasolla ilmoitettu sijainti sekä haittaohjelman katergoria ja mahdollinen alatyyppi.

## 2 Tietoturvallisuuden nykytila Suomessa

Tietoturvallisuuden yleistilanteen kartoittaminen Suomessa opinnäytetyötä aloittaessa oli monimutkainen tehtävä. Useat Tietoturvallisuusmurtojen tai rikosten kohteeksi joutuneet eri organisaatiot ovat osaltaan haluttomia tulemaan julkisuuteen tapahtuneista tietomurroista. Syinä on usein pelko esim. maineenmenetyksestä ja käyttäjien tai asiakkaiden kadosta (Piiroinen, 2015). Ongelma ei ole vain Suomea koskeva, vaan on havaittu muualla maailmassa tietomurtojen kohteiksi joutuneissa yrityksissä (Mitnick, 2005).

Monella eri julkishallinnon organisaatiolla ja yrityksellä on omia tilastotietoja sekä analyysejä tietoturvallisuustilanteesta, mutta näitä ei välttämättä lähetetä omasta organisaatiosta eteenpäin yksittäiselle organisaatiolle tai taholle joka kokoaisi niistä kokonaiskuvaa. Suurin tietoja keräävä organisaatio on Viestintävirasto joka sekä kerää omia tietojaan erinäisillä järjestelmillä kuten HAVARO:lla ja autoreporterilla että saa tietoja muilta organisaatioilta, kuten teleoperaattoreilta, joilla on lakisääteisiä velvoitteita luovuttaa tietoja sekä ilmoittaa tapahtuneista loukkauksista (Viestintävirasto, 2015).

Autoreporterin ja HAVARO:n keräämistä tiedoista näkyy että vuositasolla tapahtuu mittavaa vaihtelua sinne rekisteröityvien tapahtumien välillä. Vuonna 2013 autoreporterilla rekisteröitiin 492426 tapausta, kun vuonna 2014 rekisteröitiin vain puolet edellisestä, 217254 tapausta. Määrän väheneminen selittyy osin vuoden 2012- 2013 aikana esiin tulleiden haittaohjelmien päätyypeistä ja niihin kohdistetuista vastatoimista, sekä osin autoreporterin toimintaperiaatteesta, joka pohjautuu haittaohjelmien lähettämän liikenteen tunnistamiseen Suomalaisissa verkoissa.

Toinen selittävä tekijä laskulle on vuosina 2012 – 2013 yleistynyt uusi haittaohjelmailmiö johon kuuluvia ohjelmia yleisesti kategorisoidaan kiristysohjelmistoiksi. Niistä tunnetuimpia esimerkkejä ovat mm. Cryptolocker & Cryptowall (Viestintävirasto, 2013). Näiden haittaohjelmien luonteeseen ei kuulu muiden haittaohjelmien tapaan tiedon lähettämistä eteenpäin, vaan ohjelman päästyä tietokoneen sisään, se sulkee käyttäjän ulos, salaa sisällä olevat tiedostot ja vaatii lunnasmaksua jotta käyttäjä saa pääsyn takaisin omaan laitteeseensa. Esimerkki Cryptolocker-haittaohjelmasta näkyy kuvassa 3.

Usein bitcoin-virtuaalivaluuttana vaadittua lunnasmaksua on huomattavan vaikeaa jäljittää, jolloin toiminta on kiristysohjelmiston tekijälle taloudellisesti hyödyttävää ja riskittömämpää

kuin tavallisien tietoa keräävien ja lähettävien haittaohjelmien levittäminen. Bitcoin on digitaalinen, epävirallinen ja kansainvälinen valuutta joka perustuu verkossa tapahtuvaan kirjanpitojärjestelmään johon jokainen valuutan siirto tallentuu, ja jossa omistajien nimet on anonymisoitu (Bittiraha, 2015). Bitcoin-rahoja tyypillisesti siirretään useaan kertaan ennen jakoa toimintaan erikoistuneille rahamuuleille jotka siirtävät saamansa osan muiksi valuutoiksi, ja sen jälkeen jakavat rahat toimintaan osallistuvien henkilöiden kesken. Tämän tyyppisen rahavirran selvittäminen vie huomattavia määriä resursseja sekä aikaa poliisilta, ja ovat siksi toimintaa harjoittavien rikollisien suosimia.

Ensimmäiset versiot kiristysohjelmista lähtivät leviämään huomattavan nopeaan tahtiin, jolloin Viestintäviraston CERT-FI julkaisi ensin ohjeet haittaohjelmiston poistamiseksi, ja julkaisi hieman tämän jälkeen yhdessä Poliisin ja F-securen kanssa ransomware.fi – sivuston jonka avulla levitettiin tietoa kiristysohjelmista, kehoitettiin olla maksamatta ja annettiin ohjeita tiettyjen kiristysohjelmatyyppien poistamiseksi.


Kuva 3. Kuvakaappaus Cryptolocker - haittaohjelmasta vaatimassa saastuttamaltaan laitteen omistajalta n. 500€ maksua tietokoneen lukituksen poistamiseksi

## 2.1 Tietoturvallisuuskoulutuksen kohdentaminen

Suurin osa tietoturvallisuuteen liittyvästä koulutuksesta Suomessa kohdistuu organisaation tietohallinnon henkilöstölle sekä muille asiantuntijoille. Euroopassa ja Suomessa järjestetään tietoturvallisuuteen liittyviä lyhyitä koulutuksia, mutta kyseessä on tyypillisesti suurien organisaatioiden omat koulutusjärjestelmät joissa tietoturvallisuuskoulutus on pienenä osana uuden työntekijän perehdytystä. Tämä ei kuitenkaan sulje pois ulkoisien koulutusorganisaatioiden palveluntarjontaa sillä esimerkiksi Iso Britanniassa, Cambridgen yliopiston IT-henkilöstö oli vuonna 2015 kokeillut Futurelearn -organisaation kyberturvallisuuskurssia. Yliopiston IT-osasto oli kuitenkin päätynyt tulokseen että kurssi ei sisällä tarpeeksi käytännön harjoituksia palvellakseen yliopiston tarkoituksia (Futurelearn, 2015).

Suuremmissa organisaatioissa Suomessa työntekijöiden tietoturvallisuuteen liittyvän koulutuksen tarjoajana ovat organisaatioiden omat IT-osastot jotka saattavat järjestää myös tietoturvallisuuden kursseja henkilöstölle osana uusien työntekijöiden perehdyttämistä. Näiden organisaatioiden järjestämien omien koulutuksien ulkopuolella ei löydy koulutustarjontaa tietoturvallisuuden perusteiden kouluttamista varten käytännön työntekijätasolla, yksittäisiä ja kohdennettuja verkkokoulutuksia lukuun ottamatta. Näissäkin koulutuksissa painopiste ja koulutussisältö ovat usein organisaation määrittelemät.

Autoreporter – järjestelmän tilastojen pohjalta perustason koulutuksella yleisimpien vaarojen tunnistamiseksi voidaan merkittävästi vähentää organisaatioon kohdistuvan, tietoturvallisuuteen liittyvien toteutuvien riskien määrää ja turvata organisaation toiminnan jatkuvuutta. Toisaalta aihepiiriin liittyvä koulutus soveltuu sinällään hyvin myös yksityishenkilöiden tietoturvallisuuskurssiksi, sillä tyypillisimmät tietoturvallisuuteen liittyvät yksityishenkilöihin kohdistuvat uhat ovat usein samoja kuin organisaatioihin kohdistuvat. Käräjäoikeudesta hankittujen esimerkkitapauksien tuomiopöytäkirjat tukevat tätä näkemystä, sillä tekotavat olivat lähes poikkeuksetta kohdistettu järjestelmien perustason käyttäjiä vastaan.

## 2.2 Tietoturvallisuuteen liittyvän tilastoinnin ongelmallisuus

Poliisin tietokannoissa on mahdollisuus merkitä tutkinnassa olevia rikoksia tietoturvallisuusrikoksiksi, mutta tätä toimintoa ei toistaiseksi ole laajamittaisessa käytössä, tehden poliisin PolStat – tilastotietojen tulkinnan tästä näkökulmasta ongelmalliseksi. Tätä puutteellisuutta kasvattaa lisää sama tietoturvallisuusrikosten kohteiksi joutuneiden organisaatioiden haluttomuus lähteä tekemään tutkintapyyntöä poliisille maineenmenetyksen pelossa. Kyseessä on tyypillisesti asianomistajarikos, joten tapausta ei voi lähteä selvittämään ilman että asianomistaja haluaa tehdä asiasta rikosilmoitusta (Piiroinen, 2015).

Toinen ongelma poliisien tilastojärjestelmässä on tietoturvallisuuteen liittyvän rikollisuuden volyymi. Tavanomaisissa rikoksissa kuten ryöstöissä tai pahoinpitelyissä yksittäisen tekijän tekemien rikosten määrä on hyvin vähäinen. Vastaavasti tietoturvallisuuteen liittyvässä rikollisuudessa nämä määrät voivat olla jopa kymmentuhatkertaisia. Havainnollistavana tapauksena kokoluokista toimii Espoon käräjäoikeudessa käsitelty tapaus R 14/2613 joka tapahtui vuosina 2012–2013, jossa yksittäinen tekijä oli tuomittu usean muun eri syytekohdan lisäksi 50700, eri tietomurrosta jotka oli tehty noin kolmen kuukauden aikana. Tietomurtojen määrä on huikea verrattuna koko vuoden 2014 PolStatin tietoihin, jolloin oli tilastoitu yhteensä 339 tietomurtoa (PolStat, 2015) Lukuja vertaamalla yksittäisen tekijän toimet olisivat kasvattaneet parin kuukauden toiminnan aikana tilastoitujen tietomurtojen määrää Suomessa noin 150 - kertaisesti.

50 700 tietomurron sijasta PolStatin tilastoissa käräjäoikeuden tapaus R 14/2613, kuten useat muut, lasketaan kuitenkin vain yhdeksi tietomurtotapaukseksi. Hyvä puoli menettelyssä on se, että sen perusteella pystytään kohtuullisesti päättelemään yksittäisien toimijoiden määrän kokoluokka tilastoista, mutta yksittäisien tekijöiden tekemien tietomurtojen määrä saattaa vaihdella suuresti yksittäisistä teoista kymmeniin tuhansiin, jolloin koko rekisteristä on mahdotonta päätellä kuinka monta tietomurtotapahtumaa Suomessa tapahtuu vuositasolla. Polstatin tietoturvallisuuteen liittyvää aineistoa on näkyvillä liitteessä 4.

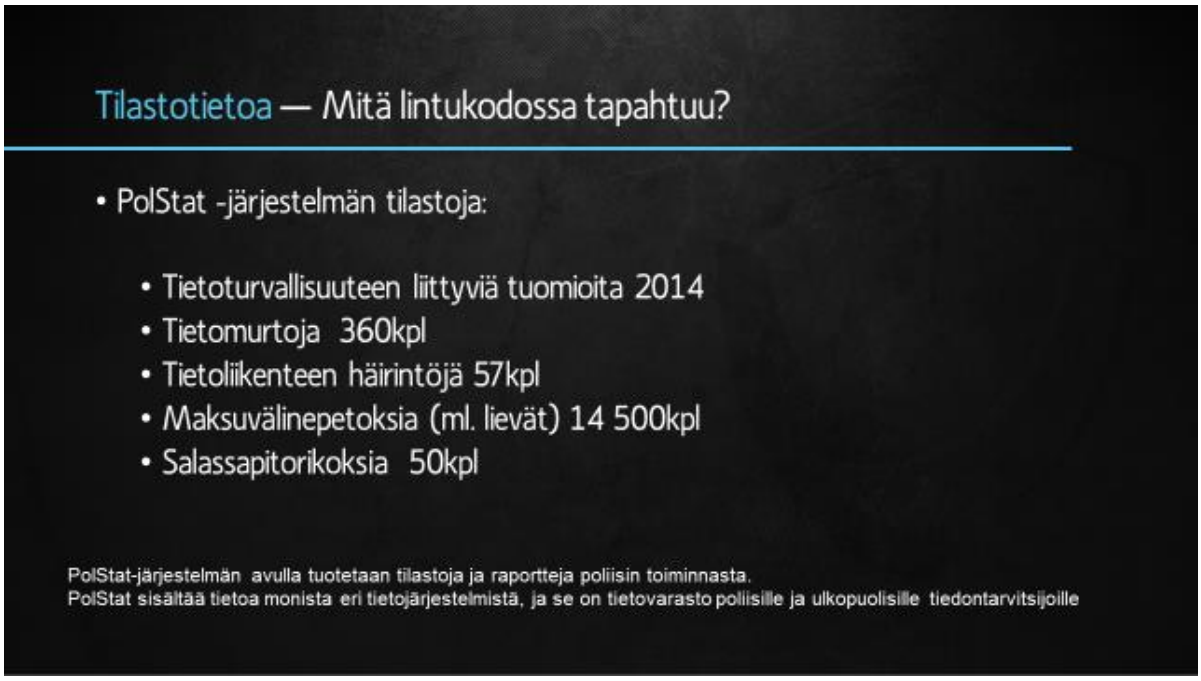
Niistä tiedoista ja tilastoista jotka ovat PolStatista saatavilla, pystytään kuitenkin selkeästi hahmottamaan että suurin osa tapahtuneista tietoturvaloukkauksista tapahtuu edelleen yksinkertaisien ja vuosikymmeniä vanhojen hyökkäystapojen avulla. Hyvänä esimerkkinä näistä toimii kalasteluviesteillä tapahtuva rikollinen toiminta, jossa kohdehenkilöille lähetetään sähköpostiin viesti joka naamioidaan näyttämään pankilta tulleelta kirjeeltä ja joka pyytää kirjautumaan pankin verkkopalveluihin erinäisillä verukkeilla kuten väärillä maksuilla tai tietoturvapäivityksillä. Viestissä oleva linkki johtaa kuitenkin usein henkilön pankin omien sivujen sijasta rikollisten omalle sivustolle joka on naamioitu kopioksi pankin sivuista. Tämä valesivusto kirjaa syötetyt kirjautumistiedot talteen, joiden avulla rikolliset pääsevät uhrin tiliin käsiksi, siirtäen uhrien tileiltä rahaa kolmannen osapuolen tilille, ja tämän osapuolen tililtä eteenpäin jaettuna tekijöiden omille tileille, kasvattaen rahavirran selvitystyötä. Oikeuslaitoksilta saaduista tuomiopöytäkirjoista ja julkisuudessa olevista uutisista käy ilmi, että toiminta on laajamittaista sekä rikollisille taloudellisesti hyvin kannattavaa.

Esimerkkitapauksena kalasteluviesteillä tapahtuvan rikollisen toiminnan tehokkuudesta voidaan pitää Helsingin käräjäoikeudessa käsiteltyä tapausta asianumero R 15/4261 jossa kolme henkilöä onnistuivat kalastelemaan vuoden sisällä lähes miljoona euroa yli 400 eri Suomalaiselta tililtä, mukana oli yksityishenkilöiden lisäksi pienyrityksien tilejä. Syytetyt saivat kuiten-

kin tuomion vain noin kolmestakymmenestä tapauksesta joihin liittyviä tilinumeroita he olivat vaihdelleet keskenään pikaviestipalvelu Skypessä, ja joiden keskustelulokit löytyivät vastaajien asuntojen ratsian ja koneiden takavarikon yhteydessä. Muiden tapahtumien osalta toteen näyttäminen jäi puutteelliseksi. Vastaavia tapauksia on kesän aikana ollut useita, ja pankit tyypillisesti varoittelevat huijausviesteistä useita kertoja vuodessa, mikä osaltaan kertoo toiminnan laajuudesta.

Rikosten selvittäminen tietoturvallisuuteen liittyvissä tapauksissa on usein vaikeaa juurikin toteen näyttämisestä johtuen ja ongelma on moniosainen. Rikoksen todentamiseen esimerkiksi kalasteluviestitapauksissa vaaditaan näyttöä henkilöiden rahasiirroista, ja epäillyn henkilön suorasta osallistumisesta näihin tilisiirtoihin, jotka ovat usein ulkomaisien palvelimien sisällä ja jotka poistuvat lokitiedoista usein ennen kuin tietojenluovutuspyyntö saadaan viranomaiskanavia pitkin asianmukaisille tahoille (Piiroinen, 2015). Toinen ongelma on lainsäädäntö joka salli vuoden 2015 kesään asti erinäisillä metodeilla kuten SQL-pistoksilla tehdyt tietomurrot lain sanamuotojen takia. SQL-pistoksella tarkoitetaan hyökkäystä jossa tietojen syöttöön liittyviä vajanaisia tarkistuksia hyväksikäyttäen pystytään syöttämään järjestelmään vahingollista tietokantakoodia tai antamaan ulkopuoliselle taholle pääsyn järjestelmään (Valtiovarainministeriö, 2008).

Porvoon käräjäoikeudessa käsitelty tapaus R 09/446 vapautti vastaajan useista tietomurtosyytteistä. Käsittelyn yhteydessä annettu tietosuojavaltuutetun lausunto 4.6.2009 ”Jos mitään suojatoimia ei ole ollut käytössä alunalkaen, voidaan rekisterinpitäjien korvausvaatimuksia tällaisten suojatoimien rakentamisesta jälkikäteen pitää perusteettomina” myös pohjusti oikeuskäytäntöä jossa toisaalta tietomurron kohteena olevan järjestelmän suojatoimien tulee olla tarpeeksi riittävät jotta tietomurron tunnusmerkistöt täyttyvät, ja että niistä aiheutuvien järjestelyjen kulut selvitystyötä tehdessä ovat korvattavissa. Yksittäisen organisaation tulee siis kyetä konkreettisesti näyttämään tietoturvallisuuden olleen hyväksyttävällä tasolla.




Kuva 4. Kuvakaappaus koulutusmateriaalista koskien PolStat -järjestelmän tilastoja

## 2.3 Lainsäädäntöön liittyvää problematiikkaa

Lainsäädännöllä on ollut vaikeuksia pysyä tietoturvallisuuteen liittyvien uhkien jatkuvan muutoksen kyydissä. Esimerkiksi tietojärjestelmään kuten palvelimeen murtautumista voidaan syyttää luvattomana käyttönä, mikä tekee PolStat – järjestelmän tiedoista vaikeita tietoturvallisuuden tilastoinnin näkökulmasta. Rikoslain 38 luku käsittelee tietoturvallisuuteen liittyvää rikollisuutta, mutta tietoturvallisuuteen liittyvissä rikoksissa usein syytteet sisältävät sekä useita toissijaisia rikosnimikkeitä että rikoslain 38 luvun ulkopuolella olevia syytekohtia, kuten 28 luvun luvaton käyttöä koskien kaapattujen laitteistojen käyttöä palvelunestohyökkäyksissä tai esim. 37 luvun 9 § maksuvälinepetoksista koskien palvelimilta kaapattuja pankkikortti- ja muita maksutietoja. Muita syytekohtia ovat mm. 35 luvun 1 § vahingonteko. Näitä pykäliä käytetään myös muihin syytteisiin, kuin pelkkään tietoturvallisuuteen. Luvaton käyttö saattaa koskea niin luvattomasti käyttöön otettua pyörää, kuin palvelunestohyökkäykseen kaapattua palvelinta. Maksuvälinepetoksissa tilanne on sama, sillä voidaan syyttää sekä väärennetyistä maksuvälineistä, tai verkkopalvelusta kaapatuista maksukorttitiedoista Polstatin järjestelmissä näitä tapauksia ei voida erottaa tietoturvallisuuteen liittyvistä tapauksista.

Myös ongelmallista tietoturvallisuuden lainsäädännössä on tietoturvallisuuteen liittyvä nopea muuttuvuus. Haittamielessä tehtyjen SQL-pistoksien olemassaolo on tiedetty pitkään, mutta laitteistojen ja palveluiden kehittyessä syntyy myös uusia tapoja käyttää erinäisiä komentoja joilla ei varsinaisesti rikota turvallisuusjärjestelyjä, vaan hyväksikäytetään järjestelmässä olevaa virhettä, jolloin lain määritelmä tietomurrosta ei mahdollisesti täyty. Esimerkki tälläi-

sestä toiminnasta on Porvoon käräjäoikeudessa käsitelty tapaus asianumero R09/446 jossa vastaaja vapautettiin tietomurtoja koskevista syytteistä sillä vastaaja oli käyttänyt syyttäjän rangaistusvaatimuksessa mainitsemaa ”vihamielistä pyyntöä” kohteena olleen sivuston palvelintietokoneelle ja päässyt siten käsiksi tietokantaan tallennettuna olleisiin käyttäjätunnus- ja salasanatietoihin. Kyseessä oli tietokantojen käyttämän SQL-komentokielen select-komento jonka sisältämää ohjelmointivirhettä hyväksikäyttäen syytetty oli päässyt tietoihin käsiksi. Porvoon käräjäoikeuden päätöksen perustelu asiasta oli, ettei toiminta ollut täyttänyt rikoslain tietomurtoa koskevaa tunnusmerkistöä, jossa edellytyksenä rikoksen tunnusmerkistön täyttymiselle on turvajärjestelyjen murtaminen.

## 2.4 Kehityskohde

Kehityskohteena oleva tietoturvallisuuskoulutus on sisällöltään peruskoulutustasoinen lyhytkoulutus, jonka pääasiallisena tavoitteena on vähentää organisaatioihin kohdistuvia uhkia tietoturvallisuuden saralla, sekä vähentää näiden seurauksia kouluttamalla henkilöstöä tunnistamaan tietomurtojen merkkejä, antamalla käytännön toimintaohjeita ja kokemuksia toimenpiteistä. Koulutuksen sisällön rajaaminen on haasteellista sillä aihealue on hyvin laaja ja vaatii seikkaperäistä aihealueiden purkamista ja käsittelyä. Toisaalta käytetyn ajan ollessa hyvin rajoitettu, tulee aihealueiden käsittelyä optimoida ja käsiteltyjä aihealueita priorisoitava huomattavasti.

Opinnäytetyön ollessa konstruktiivinen, tavoitteena oli luoda konkreettinen tuotos joka hyödyttäisi kohdeorganisaatiota (Ojasalo, Moilanen & Ritalahti, 2009). Päätös koulutusohjelman luomisesta tuli Alertum Oy:ltä, ja sisälsi koulutuksen yleispiirteen, keston, tavoitteet sekä rajauksen. Täten suurimmaksi tehtäväksi jäi itse koulutusohjelman luominen annettujen parametrien mukaisesti.

# 3 Koulutusohjelman luonti

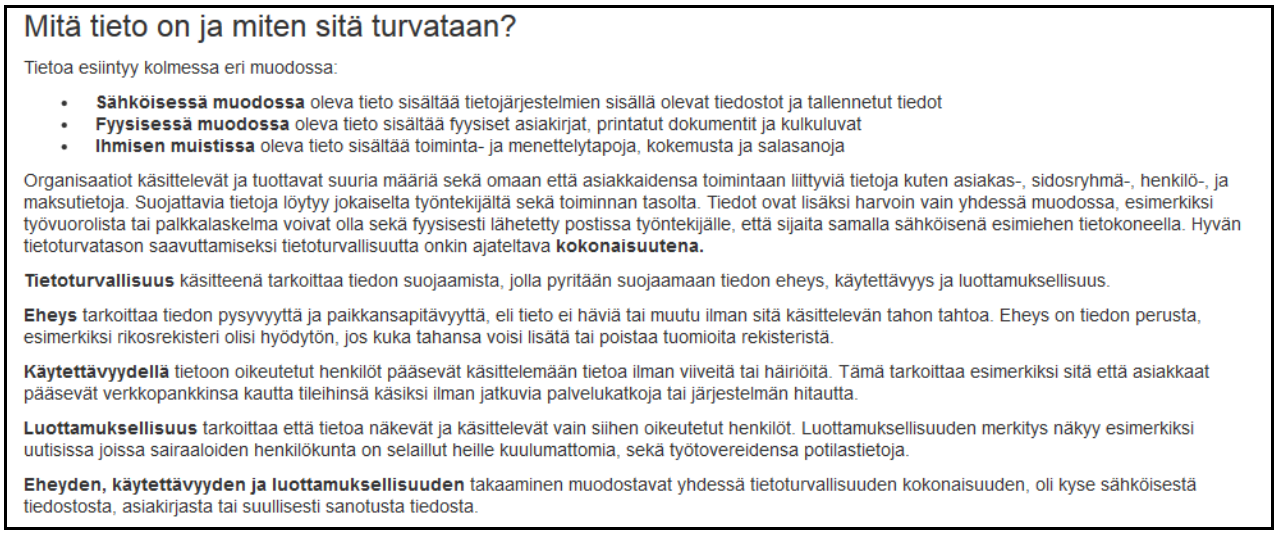
Koulutusohjelman luonti aloitettiin kesäkuussa 2015, jolloin samanaikaisesti aloitettiin myös opinnäytetyön työstäminen. Luomisprosessi oli aikataulutettu alkuperäisen suunnitelman mukaan kesäkuulta marraskuulle asti. Kesäkuussa koulutusohjelman taustaselvitystyö alkoi koulutusrungon rakentamisella sekä etsimällä lähteitä koulutuksessa käytettäviä esimerkkitapauksia varten. Näiden ohella luotiin pohjaa verkkomoduulille sekä käytännön harjoitteille. Käytännön harjoittelujen kohdalla jouduttiin jo alkuvaiheessa kuitenkin tekemään alkuperäiseen suunnitelmaan muutoksia, sillä alkuperäisenä ideana ollut jokaisen henkilön mukanaan tuoma kannettava tietokone ilmeni käytännössä joko todella rajoittavaksi tekijäksi, tai todella vaikeaksi ja kalliiksi toteuttaa.

Koulutusohjelman tavoitteet olivat moniosaiset. Toisaalta tietoturvallisuuskorttikoulutuksen tulee antaa kattava määrä tietoa hyvin teknisestä aiheesta monelta eri näkökulmalta mutta ajankäyttö on rajoitettu sillä koulutusohjelma on muodoltaan lyhytkoulutus. Muiden vastaavien koulutuksien kesto on tyypillisesti vaihdellut parista viikosta kuukausiin, mutta ovat olleet suunnattuja yksittäisille tietoturva-asiantuntijoille. Perustavaa laatua olevan tietoturvallisuuden käsitteistöksi valikoitiin sisäisen prosessin jälkeen tietoturvallisuuden määrittely, tiedon olomuodot sekä tietoturvallisuuden kolme eri lähestymistapaa. Näiden määritelmien lähteinä käytettiin Valtionhallinnon VAHTI-ohjeistusta sekä Puolustusministeriön että ulkoasiainministeriön ylläpitämää KATAKRI- kansallista auditointikriteeristöä että Valtiokonttorin Tietoturvallisuuteen liittyvää dokumentaatiota.

Monessa julkishallinnon organisaatiossa sekä liikevaihdolta ja henkilöstön lukumäärällä mitattuina suurempien organisaatioiden käytössä olevassa tietoturvallisuuteen liittyvässä materiaalissa tietoturvallisuus on määritelty suojelemaan tiedon luottamuksellisuutta, eheyttä sekä käytettävyyttä (Valtiokonttori, 2009). Muitakin ominaisuuksia on riippuen organisaatiosta ja heidän käsittelemästään tiedosta ja sen olomuodosta. Kuitenkin luottamuksellisuus, eheys ja käytettävyys ovat ominaisuuksia jotka muodostavat tietoturvallisuuden ytimen jossa

- ulkopuoliset tahot eivät pääse tietoon käsiksi
- ulkopuoliset tahot eivät pysty muokkaamaan tai poistamaan tietoa
- Tietoa käsittelevät tahot pystyvät pääsemään tietoon käsiksi

Näitä määritelmiä käytetään mm. Valtionhallinnon VAHTI-ohjeistuksessa, pohjautuen ISO 15489-standardiin koskien tietoa ja tallenteiden säilyttämistä.



## Mitä tieto on ja miten sitä turvataan?

Tietoa esiintyy kolmessa eri muodossa:

- **Sähköisessä muodossa** oleva tieto sisältää tietojärjestelmien sisällä olevat tiedostot ja tallennetut tiedot
- **Fyysisessä muodossa** oleva tieto sisältää fyysiset asiakirjat, printatut dokumentit ja kulkuluvat
- **Ihmisen muistissa** oleva tieto sisältää toiminta- ja menettelytapoja, kokemusta ja salasanoja

Organisaatiot käsittelevät ja tuottavat suuria määriä sekä omaan että asiakkaidensa toimintaan liittyviä tietoja kuten asiakas-, sidosryhmä-, henkilö-, ja maksutietoja. Suojattavia tietoja löytyy jokaiselta työntekijältä sekä toiminnan tasolta. Tiedot ovat lisäksi harvoin vain yhdessä muodossa, esimerkiksi työvuorolista tai palkkalaskelma voivat olla sekä fyysisesti lähetetty postissa työntekijälle, että sijaita samalla sähköisenä esimiehen tietokoneella. Hyvän tietoturvatason saavuttamiseksi tietoturvallisuutta onkin ajateltava **kokonaisuutena.**

**Tietoturvallisuus** käsitteenä tarkoittaa tiedon suojaamista, jolla pyritään suojaamaan tiedon eheys, käytettävyys ja luottamuksellisuus.

**Eheys** tarkoittaa tiedon pysyvyyttä ja paikkansapitävyyttä, eli tieto ei häviä tai muutu ilman sitä käsittelevän tahon tahtoa. Eheys on tiedon perusta, esimerkiksi rikosrekisteri olisi hyödytön, jos kuka tahansa voisi lisätä tai poistaa tuomioita rekisteristä.

**Käytettävyydellä** tietoon oikeutetut henkilöt pääsevät käsittelemään tietoa ilman viiveitä tai häiriöitä. Tämä tarkoittaa esimerkiksi sitä että asiakkaat pääsevät verkkopankkinsa kautta tileihinsä käsiksi ilman jatkuvia palvelukatkoja tai järjestelmän hitautta.

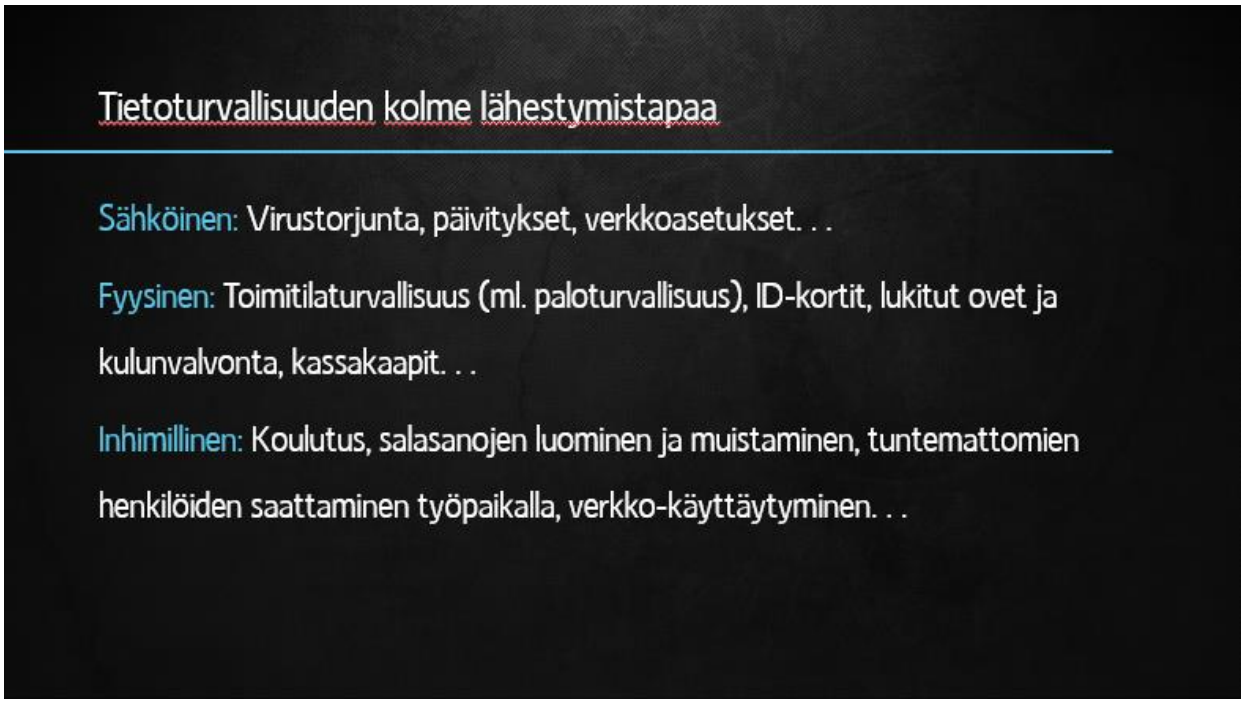
**Luottamuksellisuus** tarkoittaa että tietoa näkevät ja käsittelevät vain siihen oikeutetut henkilöt. Luottamuksellisuuden merkitys näkyy esimerkiksi uutisissa joissa sairaaloiden henkilökunta on selaillut heille kuulumattomia, sekä työtovereidensa potilastietoja.

**Eheyden, käytettävyyden ja luottamuksellisuuden** takaaminen muodostavat yhdessä tietoturvallisuuden kokonaisuuden, oli kyse sähköisestä tiedostosta, asiakirjasta tai suullisesti sanotusta tiedosta.

Kuva 5. Kuvakaappaus tietoturvallisuuskorttikoulutuksen verkkokoulutusmateriaalista, määrittäen Luottamuksellisuutta, eheyttä ja käytettävyyttä sekä tiedon olomuotoja

Tiedon olomuodoilla puolestaan kuvataan missä muodossa tietoa voi olla olemassa. Yleinen jako joka on käytössä mm. Puolustusministeriön ja ulkoasiainministeriön KATAKRI- ohjeistossa pohjautuu kolmiasteisuuteen: Sähköisessä muodossa kuten tietokoneen kovalevyllä olevaan, Fyysisessä muodossa kuten kirjana, ohjeena, muistiona tai sopimuksena olevaan ja ihmismuistissa kuten kokemuksena tai salasanana olevaan tietoon. Tietoturvallisuuden edistämiseksi ei voida näinollen keskittyä pelkkään sähköiseen tietoturvallisuuteen, vaan organisaation kaiken tiedon turvallisuuteen kokonaisvaltaisen lopputuloksen varmistamiseksi.

Ratkaisu näihin ongelmiin on yleisesti niin ikään kolmiportainen joka koostuu sähköisistä, fyysisistä ja inhimillisistä ratkaisusta. Palomuurit, ja ohjelmistopäivitykset ovat sähköisiä, lukolliset ovet ja murtohälyttimet fyysisiä, ja kouluttaminen inhimillisiä tapoja joilla suojata tietoja. Näiden kolmen eri alueen suojaamisella organisaation tietoturvallisuutta voidaan suojata tehokkaasti, vaikka se olisikin useassa eri olomuodossa ja monessa eri paikassa samanaikaisesti.




Kuva 6. Tietoturvallisuuden kolme lähestymistapaa. Kuvakaappaus lähiopetusmateriaalista.

## 3.1 Tietoturvallisuuskoulutuksen pedagoginen puoli

Tietoturvallisuuskorttikoulutuksen pedagogisen puolen taustatyössä oli mukana Alertum Oy:n koulutuspäällikkö Mika Ahola, jonka kanssa suunniteltiin koulutuksen opetuksellista näkökulmaa. erityisen tarkastelun kohteena oli kysymys siitä, kuinka koulutettavat asiat saataisiin mahdollisimman ymmärrettävästi ja selkokielisesti opetettua koulutettaville henkilöille. Koulutuksen opetuksellisessa puolessa päädyttiin nojaamaan konstruktiivista oppimiskäsitystä käsittelevään kirjaan Oppiminen ja koulutus (Rauste-von Wright, von Wright & Soini, 2003), jossa keskeisinä elementteinä toimivat oppijan motivointi, sosiaalinen vuorovaikutus, oppimisen kytkeminen toimintaan ja uusien asioiden linkittäminen jo olevaan tietoon. Käytännön tasolla tehokkaimmiksi opetusmetodeiksi tietoturvallisuuskorttikoulutuksessa ilmeni sekä pelillistäminen että toiminnallistaminen.

Pelillistämisellä opiskelijaa motivoidaan oppimaan palkitsemalla annettujen tehtävien suorittamisesta, sekä vertailemalla tuloksia muiden osallistujien kesken. Käytännössä tätä voidaan tehdä luomalla koulutusmateriaaliin erinäisiä pelimuotoisia kysymyksiä tai testejä, ja näyttämällä kurssin testitilastoja osallistujille. Opinnäytetyön aikana pelillistäminen verkkomoduulissa todettiin kuitenkin osalta liian kalliiksi toteutettavaksi budjettiin nähden, jolloin verkkomoduuli tuotettiin organisaation kumppanin luoman ratkaisun pohjalta teksti- ja kuvapohjaisena. Pelillistämisen elementtejä siirrettiin kuitenkin lähiopetukseen mm. verkkomoduulin tulosten vertailun muodossa.

Toiminnallistavassa opetusmetodissa kurssille osallistuvia henkilöitä pyritään osallistamaan koulutukseen luomalla erinäisiä toimintoja, joihin kurssilaiset osallistuvat. Alkuperäisenä ideana tämä olisi tapahtunut mm. kannettavien tietokoneiden avulla joilla kurssilaiset olisivat käyneet ohjatusti läpi tietokoneeseen ja sen käyttöjärjestelmiin liittyviä tietoturvallisuusominaisuuksia. Kannettavat tietokoneet todettiin kuitenkin käytännössä haasteelliseksi järjestelyksi, sillä jokainen kurssille osallistuva ei välttämättä sellaista ole. Muina rajoittavina tekijöinä toimivat tämän vaihtoehdon kustannukset sekä erinäisten organisaatioiden ohjeistus kannettavien tietokoneiden käsittelystä. Toisaalta tämä vaihtoehto olisi luonut logistisen ongelman jossa kouluttajat joutuisivat kantamaan mukanaan potentiaalisesti kymmeniä kannettavia tietokoneita koulutustilaisuuksia varten, sekä huolehtimaan niiden toimivuudesta ja latauksesta.

Kannettavien tietokoneiden muodostuessa haasteeksi, päädyttiin toiseen, Mobiililaitteiden avulla tapahtuvaan toiminnalliseen osioon lähiopetuksessa. Mobiililaitteiden levikki on kannettavia tietokoneita huomattavasti suurempi, ja vaihtoehtona logistisesti ja taloudellisesti huomattavasti helpompi. Näin päädyttiin lopulliseen ratkaisuun jossa käydään läpi mobiililaitteiden asetuksia sekä turvallisuusratkaisuja, että mitä tehdä jos laite katoaa tai varastetaan.

Tällä ratkaisulla pystytään toisaalta alleviivaamaan tietoturvallisuuden olevan laajempi aihealue, ja koskevan muutakin kuin varsinaisia tietokoneita, ja toisaalta vastaamaan yhä kasvavaan mobiililaitteisiin kohdistuviin tietoturvallisuusuhkiin. Tämän lisäksi toiminnallista puolta jatkettiin erinäisillä harjoitteilla joilla jo olemassa olevaa tietoa kytkettiin oppimiseen. Esimerkkinä tästä toimii salasanan muodostamiseen liittyvä harjoittelu jossa kurssilaiset muodostavat itsellensä metodeja luoda turvallisia ja muistettavia salasanoja.

### 3.2 Koulutuksen sisältö

Koulutuksen tarkka sisältö on Alertum Oy:n yrityssalaisuus eikä sitä esitellä tästä johtuen kokonaisuudessaan tai liitteenä, vaan yksittäisinä havainnollistavina liitteinä ja kuvakaappauksina tuotetusta materiaalista. Lisäksi opinnäytetyössä kerrotaan koulutuksen pääpiirteistä.

Tietoturvallisuuskorttikoulutus koostuu sekä esitäytettävästä verkkomoduulista, että lähiopetuksesta. Verkkomoduuli on noin tunnin pituinen, ja pohjautuu Alertum Oy:n kumppanin ylläpitämään ratkaisuun. Varsinainen lähiopetus on neljän tunnin pituinen. Koulutuksen sisältämät osat on esitelty liitteissä 2 ja 3 ja koulutuksen sisältöä on esitelty erillisellä tietoturvallisuuskortti.fi - sivustolla.

### 3.3 Pilottikoulutukset

Tietoturvallisuuskorttikoulutuksesta järjestettiin kaksi pilottikoulutusta 26.10.2015 sekä 29.10.2015. Ensimmäiseen pilottiin otettiin mukaan valikoituja ulkopuolisia henkilöitä yksityiseltä ja julkiselta sektorilta. Toisessa pilottikoulutuksessa oli enimmäkseen Alertum Oy:n henkilöstöä sekä tulevia tietoturvallisuuskortin kouluttajia. Nämä pilotteihin osallistuvat henkilöt kävivät läpi kurssin kokonaisuudessaan, sisältäen sekä verkko-osion että lähiopetuksen.

Kummatkin pilottikoulutukset sekä koulutusjärjestelmät sujuivat pitkälti odotuksien mukaisesti, ja osallistujien palautteet antoivat paljon hyviä ja aiheellisia jatkokehitysideoita. Pilottikoulutukset osaltaan validoivat myös koulutuksen aiheellisuuden, ja todensivat annettujen koulutuksen aikarajoitteiden olevan koulutuksen puitteisiin sopivat.

## 4 Työn arviointi

Itsereflektiona olen tyytyväinen tehtyyn työhön ja sen tuloksiin. Tämä arvio pohjautuu organisaatiolta saatuun palautteeseen sekä lähdemateriaalin ja asiantuntijahaastattelujen johtopäätöksiin. Työn ollessa työelämälle tehty projekti, oli yhteistyö kohdeorganisaation kanssa hyvin tiivis. Erityisesti yhteistyö projektin johtajana toimineen Alertum Oy:n johtavan turvallisuusasiantuntija ja osakkaan Lari Lindénin kanssa toimi tehokkaasti projektia edistäen. Tä-

män yhteistyön pohjalta Projektiin liittyvä palaute oli aiheellista ja nopeaa. Opinnäytetyön aikana luodun koulutusohjelman sisältö on osoittautunut useista eri lähteistä aiheelliseksi, sekä kohdeorganisaation puolesta hyväksi.

Negatiivisena puolena projektissa oli siihen käytetty aika joka oli jälkikäteen ajateltuna voinut olla suurempi, mutta sitä rajoittavina tekijöinä toimivat organisaation omat aikataulut sekä tavoitteet, että opiskelijan omat aikataulut.

## 4.1 Opinnäytetyön arviointi Laurean kriteeristöön peilattuna

Laurean Opinnäytetöiden arvioinnin ulottuvuudet kohdistuvat opinnäytetyössä kolmeen osa-alueeseen:

- Innovatiivisuuteen sekä käyttökelpoisuuteen
- Tutkimuksellisuuteen
- Kumppanuuteen ja autenttisuuteen

Kiitettävän arvioinnin tasossa opinnäytetyön tulisi näiden ulottuvuuksien kohdalla täyttää seuraavat kriteerit:

- Tuottaa uutta tietoa, osaamista ja muutosta
- Työelämän arvioida opinnäytetyön prosessi, ja sen tulokset selkeiksi sekä hyödyllisiksi
- Edetä johdonmukaisesti ja olla jäsennelty vakuuttavasti
- Osoittaa aiheen kannalta olennaisen tutkimuskirjallisuuden ja ammatillisen keskustelun perusteellista tuntemista
- Hallita käytettyjä tutkimus- ja kehittämismenetelmiä
- Olla toteutettu työelämän kanssa kumppanuudessa
- Olla selkeä ja aidosti työelämää kehittävä
- Omata dialoginen yhteistyösuhde eri toimijatahojen kanssa

Opinnäytetyötä reflektoiden näihin kriteereihin on pitkälti vastattu työn osissa. Varsinaista uutta tutkimustietoa ei ole opinnäytetyön aikana tuotettu, vaan kyseessä on ollut olemassa olevan tiedon jalostamisesta, eli tietoturvallisuuteen liittyvästä tilasto- ja koulutusmateriaalista tuotteeseen, jonka tavoitteena on hyödyttää työelämää. Opinnäytetyön tulokset ovat olleet kohdeorganisaatiolta tulleen palautteen pohjalta hyödylliset ja selkeät. Salassapitosopimuksien ja työn luonteen puolesta varsinaisen työn johdonmukaisuutta ei voida arvioida pelkästään tämän raportin pohjalta, sillä toinen arvioitava osa opinnäytetyötä on koulutukseen luotu liikesalaisuuden piirissä oleva materiaali.

Kohdeorganisaation puolesta tulokset ovat kuitenkin olleet johdonmukaiset, täyttäen pitkälti sille kesällä annetut tavoitteet. Käytetty aineisto on ollut ajankohtaista, monipuolista ja aiheeseen liittyen oleellista Pedagogisesta näkökulmasta materiaalia olisi voinut olla vertailua varten enemmän, mutta opinnäytetyön näkökulma ei ole arvioida koulutuksen, tai turvallisuuskoulutuksen eri pedagogisien menetelmien tehokkuutta. Tämän sijaan valittu pedagoginen lähestymistapa on valittu nojautuen kohdeorganisaation omiin kokemuksiin ja käytäntöihin. Käytettyä tutkimusmenetelmää oli opinnäytetyön aikarajoitteista johtuen jouduttu osittain soveltamaan, mutta on tuloksien arvioinnin ja kehityskohteen osia lukuun ottamatta konstruktiivisen opinnäytetyön mukainen.

Käytetty materiaali oli kattava ja monipuolinen. Lähdemateriaali oli yksityiskohtaisesti selostettua ja pohti tietoturvallisuutta useista eri näkökulmista, kuten lainopillisesta, organisaatiollisesta sekä tekijän että kohteena olevan organisaation henkilöstön näkökulmista. Myös haastateltavat henkilöt olivat tarkoituksenmukaisesti ja selvästi valikoituja keskusrikospoliisista sekä viestintävirastosta. Tarkoituksena oli myös haastatella kihlakunnan syyttäjää Jani Jukkaa ja asianajaja Markku Fredmania, mutta projektin aikataulutuksen puolesta näitä haastatteluja ei ehditty toteuttaa. Työn ollessa valmis, arvioisin kokemuksen kautta tuloksen voineen olla parempi kasvatettujen aikamääreiden myötä. Toissijaisena arviona opetuksen pedagogiseen puoleen olisi voinut keskittää myös enemmän taustakartoitusta.

Opinnäytetyön on arvioinut Alertum Oy:n osakas ja johtava turvallisuusasiantuntija Lari Lindén jonka työelämän vaikuttavuusarvio opinnäytetyöstä on tässä raportissa liitteessä neljä.

## 4.2 Jatkokehitysaiheita Tietoturvallisuuteen liittyen

Useita kehitystä kaipaavia aihealueita ilmeni projektin edetessä. Tietoturvallisuudesta syytettyjen vastaajien samoista toimista saamien tuomioiden varianssi oli huomattava, ja tuomioissa itsessään vedottiin joissain tapauksissa yli kymmenen vuotta vanhoihin ennakkotapauksiin. Syytteissä on myös huomattava määrä toissijaisia syytekohtia sillä olemassa olevaa oikeuskäytäntöä tietoturvallisuusrikollisuudesta ei ole (Länsi-Uudenmaan syyttäjänvirasto, 2015). Verrokkitapauksina toimii KKO:n ennakkotapaus 2003:36 jossa nuori mies tuomittiin pankin palvelimiin kohdistuneesta porttiskannaamisesta mittavampaan rangaistukseen kuin kalasteluviestien avulla pankkitilejä ryöstäneet henkilöt. Toisaalta myös henkilön teon tahallisuutena pidettiin henkilön asiantuntijaroolia, vaikka henkilö tekohetkellään ei omannut mitään alan koulutusta tai työtaustaa. Jatkotutkimuksen aiheena tietoturvarikosten oikeuskäytäntöjen selvittely tehostaisi ja oikeudenmukaistasi tietoturvarikollisuuden käsittelyä sekä selkeyttäisi oikeuskäytäntöjä.

Toisena opinnäytetyön aikana ilmenneenä jatkokehitysaiheena on jatkuvasti kasvava verkkoon kytkeytyvien laitteiden määrä. Tietoturvallisuuden merkitys on selkeä verkkoon kytkeytyvien laitteistojen kohdalla, ja usein puutteellinen. Esimerkiksi verkkoon kytkettyjen tulostimien välimuistista on mahdollista kaivaa tulostettuja tiedostoja, IP-kameroiden kuvaa on mahdollista nähdä joissain tapauksissa ilman että laitteisto pyytää katsojalta salasanaa (FTC, 2013). Salasanattoman kamerajärjestelmän katseleminen on myös laillisesti harmaata aluetta, sillä tietomurron tunnusmerkistön täyttämiseksi tulisi ensin murtautua järjestelmään. Toisaalta myös luvaton käyttö ei välttämättä tule kyseeseen, sillä vastaavanlaisia, julkisia järjestelmiä on olemassa mm. riistakameroiden ja kaupunkikameroiden muodossa. Ainoa konkreettisesti tunnusmerkistöt täyttävä toiminto olisi jos kamera kuvaisi asumistiloja, jolloin kotirauhan häirinnän tunnusmerkistö täyttyisi. Määritelmien selventäminen ja kehitys aiheesta voisi konkreettisesti parantaa monen organisaation ja yrityksen tietoturvallisuutta.

Lähteet

**Kirjalliset lähteet**

Airaksinen, T. & Vilkka, H. 2004. Toiminnallinen opinnäytetyö. Helsinki: Tammi

Heinonen, J. Keinänen, A. & Paasonen, J. 2013. Turvallisuustutkimuksen tekeminen. Helsinki: Tietosanoma.

Hopkin, P. 2013. Fundamentals of risk management. Understanding, evaluating and implementing effective risk management.

Kasanen, E. Lukka, K. & Siitoinen, A. 1991. Konstruktiivinen ote liiketaloustieteessä. Liiketaloudellinen aikakausikirja.

Mitnick, K & Simon, W. 2005. The art of intrusion.

Ojasalo, K. Moilanen, T. & Ritalahti, J. 2010. Kehittämistyön menetelmät. WSOYpro Oy

Rauste-von Wright, K. von Wright, J & Soini, T. 2003. Oppiminen ja koulutus. Sanoma Pro.

**Haastattelut**

Hämäläinen, Y. Erityisasiantuntijan haastattelu, 27.10.2015. Viestintävirasto. Nurmijärvi

Lindeborg, K. Rikostarkastajan haastattelu 29.7.2015. Keskusrikospoliisi. Vantaa

Piiroinen, T. Kyberrikostorjuntayksikön päällikön haastattelu 29.7.2015. Keskusrikospoliisi. Vantaa

**Tuomiopöytäkirjat**

Espoon käräjäoikeus. Asianumero R 15/268. 7.7.2015. Kihlakunnansyyttäjä Jani Jukka

Helsingin käräjäoikeus. Asianumero R 15/4261. 14.7.2015. Kihlakunnansyyttäjä Tuomas Soosalu

Porvoon käräjäoikeus. Asianumero R 09/446. 18.9.2009. Kihlakunnansyyttäjä Jani Jukka

**Sähköiset lähteet**

Alertum Oy. Tietoturvallisuus-korttikoulutus™. Viitattu 27.10.2015
http://www.tietoturvallisuuskortti.fi/

Bittiraha. Mikä on Bitcoin? Viitattu 17.11.2015

https://bittiraha.fi/content/mik%C3%A4-bitcoin

Federal Trade commission. Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy. 2013. Viitattu 3.11.2015 https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles

Futurelearn. Introduction to cybersecurity. Viitattu 27.10.2015 https://www.futurelearn.com/courses/introduction-to-cyber-security

Huoltovarmuuskeskus. HAVARO turvaa yhteiskunnan huoltovarmuuskriittisiä toimintoja. Marjo Rautvuori. 10.5.2014. Viitattu 12.11.2015 http://www.varmuudenvuoksi.fi/aihe/huoltovarmuuden_toteutuksia/106/havaro_turvaa_yhteiskunnan_huoltovarmuuskriittisia_toimintoja

Helsingin Sanomat. Huhtanen, J. Kylmän sodan kuuma linja kulki Suomen läpi – tarkka reitti yhä salassa. Viitattu 27.10.2015 http://www.hs.fi/kotimaa/a1443237269958

Helsingin Sanomat. Lehtinen T, Sjöholm, J & Halminen, L. Supo tutkii verkkohyökkäystä ulkoministeriöön törkeänä vakoiluna. Viitattu 28.10.2015 http://www.hs.fi/kotimaa/a1383191714911

(ISC)$^2$. CISSP® - Certified Information Systems Security Professional. Viitattu 5.11.2015 https://www.isc2.org/cissp/default.aspx

Länsi-Uudenmaan syyttäjänvirasto. Syytteet nostettu laajassa tietoverkkorikosten sarjassa. 11.2.2015. Viitattu 28.10.2015 http://www.oikeus.fi/syyttaja/lansi-uudenmaansyyttajanvirasto/text/fi/index/tiedotteet/2015/02/syytteetnostettulaajassatietoverkkorikostensarjassa.html

Poliisiammattikorkeakoulu. Poliisin tilastopalvelu. Viitattu 12.11.2015 http://www.polamk.fi/tki/tilastopalvelu

Puolustusministeriö. KATAKRI 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 5.11.2015 http://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/KATAKRI_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

Trinity College. Savarese, C & Hart, B. The Caesar cipher. Viitattu 27.10.2015
http://www.cs.trincoll.edu/~crypto/historical/caesar.html

Valtionhallinnon tietoturvallisuuden johtoryhmä. Johdon tietoturvaopas. 2011. Viitattu 27.10.2015
https://www.vahtiohje.fi/c/document_library/get_file?uuid=6068ca18-6214-4244-8ce6-dffe952e3e8e&groupId=10128&groupId=10229

Valtionhallinnon tietoturvallisuuden johtoryhmä. Pietikäinen, S. Tietoturvallisuus, mitä se on? 2013. Viitattu 27.10.2015
https://www.vahtiohje.fi/web/guest/691

Valtiokonttori. Tietoturvapolitiikan mallipohja. Viitattu 5.11.2015
http://www.valtiokonttori.fi/download/noname/%7B3B7C8612-9254-4AA3-9F25-A8D520955D4B%7D/84888

Valtion tieto- ja viestintätekniikkakeskus. Valtorin kokonaisvaltaisen riskienhallinnan ja kokonaisturvallisuuden toteuttaminen. Rousku, K. 30.10.2014. Viitattu 3.11.2015
http://www.valtori.fi/download/noname/%7B636334B9-1859-40EC-AB88-4EDB20FC61DF%7D/11574

Valtiovarainministeriö. VAHTIn rakenteisen verkkosivuston ensimmäinen versio. Viitattu 5.11.2015
https://www.vahtiohje.fi/web/guest

Valtiovarainministeriö. Valtiohallinnon tietoturvasanasto. 2008. Viitattu 18.11.2015
https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto

Viestintävirasto. Haittaohjelma vangitsee tietosi. 11.11.2013. Viitattu 9.11.2015
https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2013/11/ttn201311111451.html

Viestintävirasto. Viestintävirastolle tehtävät ilmoitukset. 2013. Viitattu 28.10.2015
https://www.viestintavirasto.fi/kyberturvallisuus/sahkoinentunnistaminenjaallekirjoitus/viestintavirastolletehtavatilmoitukset.html

Viestintävirasto & Huoltovarmuuskeskus. Tietoturva nyt! – seminaari. 4.11.2015. Viitattu 4.11.2015
https://www.viestintavirasto.fi/viestintavirasto/ajankohtaista/2015/seuraasuoranatietoturvanyt-seminaariakeskiviikkona4.11.2015.html

Viestintävirasto. [Teema] Autoreporter - tehokas työkalu haittaohjelmien torjunnassa. 19.3.2015. Viitattu 4.11.2015 https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/03/ttn201503191128.html

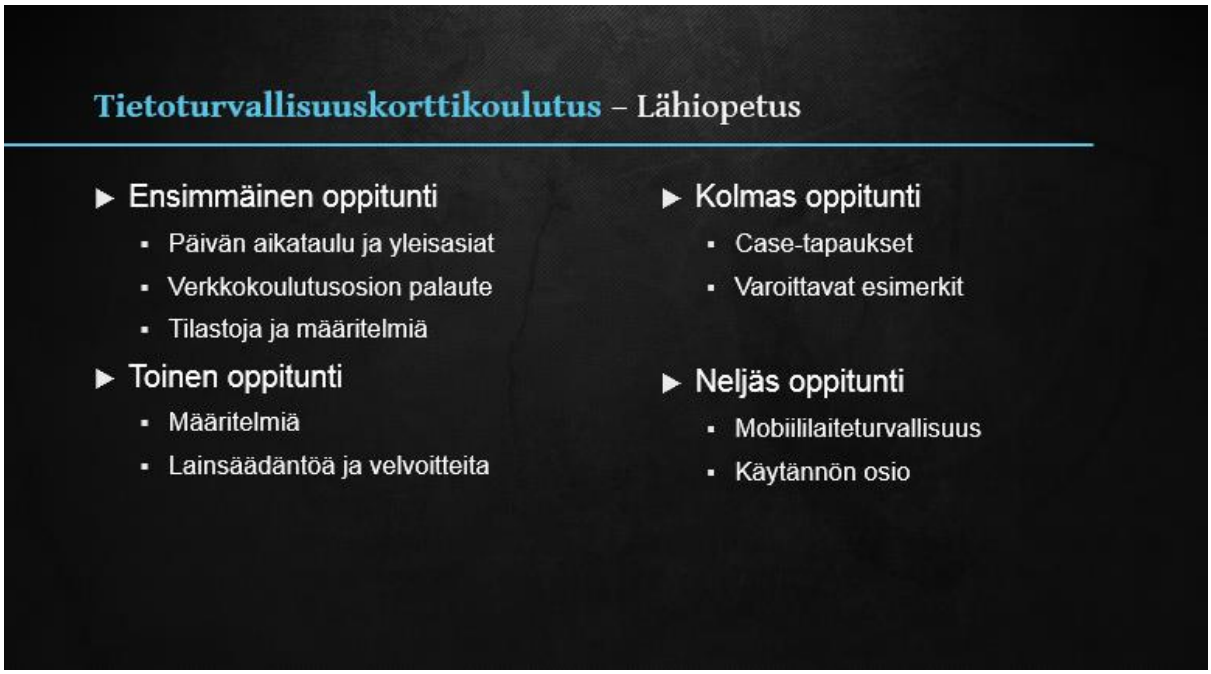
Kuvat

Liitteet

Liite 1 Verkkomoduulin aihealueiden lista.

1. Etusivu
    1.1. Tervetuloa
    1.2. Ohjeet
2. Tieto & Tietoturvallisuus
    2.1. Johdanto
    2.2. Miksi tietoturvallisuus on tärkeää
    2.3. Mitä tieto on ja miten sitä turvataan
    2.4. Välikysely
    2.5. Yhteenveto
3. Tietoturvallisuuden osa-alueet
    3.1. Johdanto
    3.2. Henkilöstöturvallisuus
    3.3. Fyysinen turvallisuus
    3.4. Tietoaineistoturvallisuus
    3.5. Välikysely
    3.6. Tietoliikenneturvallisuus
    3.7. Laitteistoturvallisuus
    3.8. Ohjelmistoturvallisuus
    3.9. Välikysely
    3.10. Yhteenveto
4. Turvalliset toimintatavat
    4.1. Johdanto
    4.2. Salasanat
    4.3. Internet
    4.4. Sähköposti
    4.5. Välikysely
    4.6. Etätyö
    4.7. Yhteisöpalvelut
    4.8. Sosiaalinen manipulointi
    4.9. Välikysely
    4.10. Yhteenveto
    4.11. Vain lopputesti jäljellä
5. Lopputesti

Liite 2 Lähiopetuksen diasarjasta otettu ohjelmarungon kuvakaappaus.



Liite 3 PolStatin tietoturvallisuuteen liittyvää rikostilastoa vuosilta 1997-2015.

Rikos
Poliisiyht

| Ilmoitettu Kpl | 1997 | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | Vuosi |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| TIETOMURRON YRITYS | 6 | 337 | 12 | 45 | 10 | 22 | 19 | 8 | 7 | 5 | 8 | 4 | 7 | 8 | 11 | 11 | 5 | 14 | 37 | **576** |
| TIETOMURTO | 31 | 37 | 35 | 37 | 47 | 89 | 77 | 83 | 110 | 112 | 139 | 183 | 140 | 292 | 410 | 503 | 580 | 339 | 137 | **3 381** |
| TÖRKEÄ TIETOMURTO | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 8 | 14 | 5 | 6 | 1 | **35** |
| LIEVÄ MAKSUVÄLINEPETOS | 172 | 160 | 161 | 176 | 208 | 226 | 321 | 283 | 338 | 375 | 372 | 406 | 442 | 448 | 458 | 548 | 788 | 946 | 462 | **7 290** |
| MAKSUVÄLINEPETOKSEN VALMISTELU | 4 | 5 | 5 | 4 | 3 | 3 | 10 | 8 | 3 | 3 | 6 | 6 | 15 | 10 | 13 | 19 | 19 | 22 | 6 | **170** |
| MAKSUVÄLINEPETOS | 2 779 | 3 011 | 2 732 | 2 745 | 2 845 | 3 064 | 3 112 | 2 966 | 3 009 | 2 649 | 2 915 | 3 026 | 4 307 | 3 876 | 5 053 | 5 546 | 6 690 | 6 699 | 2 811 | **69 835** |
| TÖRKEÄ MAKSUVÄLINEPETOS | 86 | 55 | 91 | 46 | 79 | 47 | 116 | 122 | 117 | 90 | 89 | 130 | 184 | 124 | 147 | 126 | 122 | 123 | 63 | **1 963** |
| LIEVÄ PETOS | 3 302 | 3 486 | 3 413 | 3 754 | 3 651 | 3 739 | 4 001 | 4 216 | 4 365 | 4 639 | 5 083 | 5 852 | 5 869 | 5 880 | 6 433 | 7 144 | 8 053 | 8 125 | 3 783 | **94 788** |
| PETOS | 6 518 | 6 158 | 5 541 | 6 330 | 5 625 | 6 304 | 5 481 | 5 566 | 6 340 | 6 367 | 7 090 | 8 218 | 9 552 | 7 865 | 9 026 | 11 092 | 11 232 | 10 777 | 4 678 | **139 820** |
| TYÖELÄKEVAKUUTUSMAKSUPETOS | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 7 | 3 | 11 | 15 | 22 | 11 | 9 | 5 | **90** |
| TÖRKEÄ PETOS | 439 | 421 | 540 | 1 162 | 630 | 503 | 628 | 615 | 831 | 690 | 625 | 819 | 881 | 806 | 1 027 | 864 | 958 | 1 208 | 507 | **14 154** |
| TÖRKEÄ TYÖELÄKEVAKUUTUSMAKSUPE | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 11 | 13 | 12 | 13 | 25 | 22 | 30 | 1 | **127** |
| VAKUUTUSPETOS | 9 | 11 | 8 | 10 | 21 | 6 | 10 | 8 | 6 | 5 | 6 | 7 | 6 | 5 | 5 | 3 | 5 | 7 | 4 | **142** |
| LIEVÄ VEROPETOS | 50 | 75 | 78 | 184 | 172 | 135 | 79 | 55 | 35 | 56 | 35 | 27 | 19 | 26 | 22 | 30 | 24 | 16 | 7 | **1 125** |
| TÖRKEÄ AVUSTUSPETOS | 5 | 8 | 6 | 7 | 9 | 6 | 4 | 11 | 7 | 6 | 8 | 7 | 4 | 5 | 8 | 14 | 9 | 17 | 6 | **147** |
| TÖRKEÄ VEROPETOS | 401 | 314 | 267 | 290 | 285 | 576 | 274 | 318 | 390 | 355 | 434 | 461 | 358 | 228 | 312 | 332 | 318 | 324 | 143 | **6 380** |
| TÖRKEÄ VELALLISEN PETOS | 70 | 83 | 45 | 61 | 47 | 39 | 48 | 32 | 42 | 54 | 59 | 25 | 43 | 31 | 20 | 25 | 23 | 28 | 6 | **781** |
| VELALLISEN PETOS | 153 | 140 | 107 | 90 | 69 | 66 | 50 | 42 | 48 | 43 | 34 | 37 | 35 | 27 | 30 | 22 | 26 | 24 | 5 | **1 048** |
| AVUSTUSPETOS | 53 | 26 | 72 | 38 | 28 | 23 | 27 | 42 | 33 | 29 | 31 | 20 | 28 | 37 | 27 | 29 | 13 | 13 | 3 | **572** |
| VEROPETOS | 444 | 398 | 436 | 325 | 311 | 370 | 210 | 272 | 167 | 202 | 159 | 155 | 170 | 93 | 107 | 135 | 119 | 110 | 36 | **4 219** |
| **Yhteensä** | **14 522** | **14 725** | **13 543** | **15 304** | **14 040** | **15 224** | **14 467** | **14 647** | **15 848** | **15 680** | **17 094** | **19 401** | **22 082** | **19 785** | **23 145** | **26 504** | **29 082** | **28 837** | **12 707** | **346 643** |

26.6.2015 - 1 - 13:53:50

Liite 4 Johtavan turvallisuusasiantuntijan ja osakkaan Lari Lindénin työelämän vaikuttavuus-arvio.

ALERTUM
Osaaminen luo turvan.

1 (1)

12.11.2015

**Lausunto opinnäytetyöhön**

Leo Hämäläinen on toteuttanut opinnäytetyönsä työelämälähtöisesti Alertum Oy:n tuotekehitysprojektissa.

Tuotekehityksen lopputuotteena on tietoturvallisuuden perustason koulutus, joka on toimialariippumaton ja kaikille soveltuva. Koulutus koostuu ennakkoon tehtävästä verkkokoulutusosiosta sekä neljän tunnin lähiopetuksesta. Koulutus tulee markkinoille joulukuussa 2015.

Hämäläisellä on ollut projektissa keskeinen rooli muun muassa taustaselvitysten tekemisessä sekä koulutusaineiston luomisessa. Allekirjoittanut johti projektin ja toimi opiskelijan ohjaajana.

Hämäläinen suoriutui tehtävästään kiitettävästi, toimi tavoitteellisesti, osoitti hyvää projektinhallintakykyä sekä vahvaa tietoturvallisuus-osaamista.

**Lari Lindén**
Johtava turvallisuusasiantuntija, osakas
Alertum Oy